RFC 7027 : Elliptic Curve Cryptography (ECC) Brainpool Curves for Transport Layer Security (TLS)

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 3 octobre 2013. Dernière mise à jour le 21 mai 2014

Date de publication du RFC : Octobre 2013

https://www.bortzmeyer.org/7027.html

Rien d'extraordinaire dans ce très court RFC : juste l'enregistrement de trois nouvelles courbes elliptiques, collectivement nommées Brainpool, pour utilisation dans TLS.

Ces courbes Brainpool avaient été normalisées originellement dans le RFC 5639 [1] (et leur description était dans « *"ECC Brainpool Standard Curves and Curve Generation - v. 1.0"* <http://www.ecc-brainpool.org/download/Domain-parameters.pdf> »). Le protocole TLS permet d'utiliser des courbes elliptiques depuis le RFC 4492. Ces trois courbes Brainpool avaient déjà des OID mais TLS nécessitait en plus l'enregistrement de noms, ce qui est désormais fait.

Les trois courbes sont ainsi nommées, avec la syntaxe de TLS :

```
enum {
            brainpoolP256r1(26),
            brainpoolP384r1(27),
            brainpoolP512r1(28)
      } NamedCurve;
```

Et elles figurent désormais dans le registre IANA <https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml#tls-parameters-8>.

Au fait, pourquoi de nouvelles courbes elliptiques alors qu'il y en a déjà plein, dont certaines normalisées par le NIST ? C'est parce qu'il existe de sérieux soupçons que les courbes NIST aient été délibérement affaiblies sur ordre de la NSA (voir l'exposé « *"Crypto Won't Save You Either"* <http://regmedia.co.uk/2014/05/16/0955_peter_gutmann.pdf> », p. 73).

Pour ceux qui lisent la langue de Konrad Zuse, il existe un site Web sur Brainpool en allemand <http://www.ecc-brainpool.org>.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc5639.txt